

**IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES**

UNITED STATES,)	AMICUS CURIAE BRIEF OF
<i>Appellant,</i>)	NOTRE DAME LAW STUDENT
)	IN SUPPORT OF APPELLEE
v.)	
)	USCA Dkt. No. 17-0153/AR
Sergeant (E05),)	Crim. App. No. 20150776
EDWARD J. MITCHELL II, USA,)	
<i>Appellee.</i>)	

**TO THE HONORABLE JUDGES OF THE UNITED STATES COURT OF
APPEALS FOR THE ARMED FORCES:**

Dominic X. Barceleau, a law student at the Notre Dame Law School, and his supervising attorney, Professor Stephen F. Smith, respectfully submit this amicus curiae brief in support of Appellee by invitation of the Court pursuant to this Court's Rule 26(a).

STEPHEN F. SMITH
Professor of Law
Notre Dame Law School
Notre Dame, IN 46556
(574) 631-3097
ssmith31@nd.edu

DOMINIC BARCELEAU
J.D. Candidate
Notre Dame Law School
Notre Dame, IN 46556
(781) 910-9477
dbarcele@nd.edu

Counsel for Amici Curiae

INDEX OF BRIEF

INDEX OF BRIEF	ii
TABLE OF AUTHORITIES	iv
ISSUE PRESENTED	1
STATEMENT OF STATUTORY JURISDICTION.....	1
STATEMENT OF THE CASE.....	1
STATEMENT OF FACTS.....	1
STATEMENT OF INTEREST.....	1
INTRODUCTION.....	2
ARGUMENT	3
I. FORCING APPELLEE TO RECALL FROM MEMORY AND DISCLOSE HIS SECRET PASSWORD CONSTITUTED COERCED TESTIMONY	5
A. <i>Just As Disclosure from Memory of the Combination to a Locked Safe Is Testimonial, So, Too, Is Recall and Disclosure of the Password to a Locked Electronic Device</i>	8

<p>B. <i>It is Irrelevant that Appellee Did Not Explicitly Disclose His Passcode Through Spoken or Written Word Because Entering the Code Directly into the iPhone Produced the Same Testimonial Result</i></p>	14
<p>II. DECRYPTION OF ENCRYPTED DEVICES OR MEDIA IS TESTIMONIAL BECAUSE IT RECREATES ON THE UNENCRYPTED DEVICE CONTENT THAT OTHERWISE EXISTS ONLY IN THE ACCUSED’S MIND.....</p>	18
<p>III. THE FORCED DISCLOSURE OF APPELLEE’S SECRET PASSWORD AND FORCED DECRYPTION OF HIS LOCKED IPHONE WAS INCRIMINATING</p>	21
<p>CONCLUSION.....</p>	24

TABLE OF AUTHORITIES

United States Supreme Court

<i>Doe v. United States</i> , 487 U.S. 201 (1988).....	passim
<i>Fisher v. United States</i> , 425 U.S. 391 (1976)	8
<i>Hiibel v. Sixth Judicial District Court of Nevada</i> , 542 U.S. 177 (2004)	10
<i>Hoffman v. United States</i> , 341 U.S. 479 (1951)	11
<i>Kastigar v. United States</i> , 406 U.S. 441 (1972)	26
<i>Maness v. Meyers</i> , 419 U.S. 449 (1975)	11
<i>Pennsylvania v. Muniz</i> , 496 U.S. 582, (1990)	7
<i>Schmerber v. California</i> , 384 U.S. 757 (1966)	11
<i>United States v. Doe</i> , 465 U.S. 605 (1984)	10
<i>United States v. Hoffman</i> , 341 U.S. 479 (1951)	26
<i>United States v. Hubbell</i> , 530 U.S. 27 (2000)	passim

United States Courts of Appeal

<i>In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011</i> , 670 F.3d 1335 (2011)	24, 26, 27
<i>United States v. Green</i> , 272 F.3d 748 (5th Cir. 2001)	21, 22

United States District Courts

<i>In re Boucher</i> , No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009)	24
--	----

<i>SEC v. Huang</i> , No. 15-269, 2015 WL 5611644 (E.D. Pa. Sept. 23, 2015).....	16
<i>United States v. Fricosu</i> , 841 F. Supp. 2d 1232 (D. Colo. 2012).....	24
<i>United States v. Kirschner</i> , 823 F. Supp. 2d 665 (E.D. Mich. 2010)	16

State Courts

<i>Commonwealth v. Gelfgatt</i> , 11 N.E. 3d 605 (Mass. 2014).....	24
<i>Florida v. Stahl</i> , 206 So. 3d 124, (Fla. Dist. Ct. App. 2016).....	15

ISSUE PRESENTED

I. WHETHER THE FIFTH AMENDMENT'S SELF INCRIMINATION CLAUSE IS VIOLATED WHEN A SUSPECT VOLUNTARILY UNLOCKS HIS IPHONE WITHOUT GIVING HIS PERSONAL IDENTIFICATION NUMBER TO INVESTIGATORS.

STATEMENT OF STATUTORY JURISDICTION

Appellee's Statement of Statutory Jurisdiction is accepted.

STATEMENT OF THE CASE

Appellee's Statement of the Case is accepted.

STATEMENT OF FACTS

Appellee's Statement of Facts is accepted.

STATEMENT OF INTEREST

Barceleau attended college on a four-year Army R.O.T.C. scholarship and is a member of the Army Individual Ready Reserve until he begins his active service as a member of the Army JAG Corps after graduating from Notre Dame in 2018. Smith served during college and law school as an enlisted member of the Navy Reserve. Both amici are keenly interested in ensuring that the constitutional rights of those who defend our freedoms as uniformed members of the armed forces are fully protected and appreciate this opportunity to be of service to the Court.

INTRODUCTION

Try as Appellant and its amici might to create the opposite impression, this is a fairly straightforward case calling for suppression of unconstitutionally obtained evidence. The military judge carefully considered the evidence and governing law and found that military investigators illegally compelled Appellee to give incriminating testimony against himself—and, even worse, persisted in doing so even *after* Appellee had clearly invoked his constitutional right not to submit to interrogation without the presence of counsel. The judge’s decision was eminently correct and well supported by the record evidence. It should be affirmed.

The Fifth Amendment privilege against self-incrimination—the sole issue we address—was plainly violated by the government’s determined effort to conscript Appellee into helping it prove what it evidently viewed as an otherwise unwinnable case against him. “At its core, the privilege reflects [our nation’s] fierce ‘unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt’”—an inquisitorial practice which “defined the operation of the Star Chamber.” *Pennsylvania v. Muniz*, 496 U.S. 582, 596 (1990) (quoting *Doe v. United States*, 487 U.S. 20, 212 (1988)).

This is *exactly* the situation the government foisted upon Appellee here. In the face of repeated demands by interrogators that he recall from memory and disclose his iPhone password, Appellee faced the “cruel trilemma” the Privilege

forbids: he could *disclose* his secret password (and thereby furnish an essential link in the chain of evidence needed to convict him), *lie* and say that he did not know (or could not remember) the password, or *refuse to obey* the investigators' direction, who were at that time keeping him detained in his company commander's office. The government's strong-armed tactics thus compelled Appellee to be a "witness against himself" in violation of the Fifth Amendment.

ARGUMENT

Much of the discussion in the briefs in this case focus on the "act of production" doctrine. The doctrine applies when, instead of being required to disclose *information*, by word or deed, which could furnish a link in the chain leading to conviction, the accused is compelled to produce *documents or other physical evidence*. *United States v. Hubbell*, 530 U.S. 27, 35 (2000). Although the incriminating nature of items of physical evidence cannot be used to defeat a production order (because "the[ir] creation . . . was not 'compelled,'" *id.*), the doctrine accords Fifth Amendment protection to any factual assertions, express or implied, contained in the act of producing the evidence under compulsion. *Id.* at 36–37; *see also, e.g., Fisher v. United States*, 425 U.S. 391, 410 (1976) ("The act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the papers produced.").

Although the act-of-production doctrine has proven difficult to apply in some cases—and is regarded by some as insufficiently protective of legitimate self-incrimination concerns, *see, e.g., Hubbell*, 530 U.S. at 49 (Thomas, J., concurring)¹—Appellee has a compelling argument under the doctrine. As Appellee and amicus ACLU and Electronic Frontier Foundation convincingly show, the majority of reported federal decisions have ruled that the act of producing an unlocked and decrypted password-protected device containing incriminating evidence is “testimonial” and thus protected against compulsory process by the Fifth Amendment. *See* Appellee’s Answer 17–25; Br. of EFF and ACLU as Amici Curiae in Supp. of Appellee 11–17.

In this brief, we seek to alert the Court to an equally compelling self-incrimination ground for affirmance independent of the act-of-production doctrine. In our view, forcing Appellee to disclose his secret password for entry into his mobile device was, in itself, “communicative” or “testimonial” in nature. This conclusion is strengthened by the fact that compelled disclosure of the password and entry into the locked iPhone entailed decrypting the device’s contents, thereby

¹ In *Hubbell*, Justice Thomas argued that, contrary to the limited scope of the act-of-production doctrine, “[a] substantial body of evidence suggests that the Fifth Amendment privilege protects against the compelled production not just of incriminating *testimony*, but of any incriminating *evidence*.” 530 U.S. at 49 (emphasis added). On this view, Appellee would undeniably win based on the incriminating nature of the decrypted files retrieved from his iPhone.

recreating on the device information which otherwise existed only in the recesses of Appellee's mind. Each of these testimonial acts—namely, disclosing the secret password, and decrypting the illegible files contained on the iPhone—formed links (and, indeed, *essential* links) in the chain of evidence leading to the incriminating content reproduced in the unlocked and decrypted device. Nothing more is required to conclude that the evidence the government obtained through Appellee's coerced disclosures, and could not otherwise have obtained, was properly suppressed on Fifth Amendment grounds.

I. FORCING APPELLEE TO RECALL FROM MEMORY AND DISCLOSE HIS SECRET PASSWORD CONSTITUTED COERCED TESTIMONY.

Unlike the more involved analysis required under the act-of-production doctrine, the analysis of other Fifth Amendment issues is fairly straightforward. “The Self-Incrimination Clause reflects a judgment . . . that the prosecution should [not] be free to build up a criminal case, in whole or in part, with the assistance of enforced *disclosures* by the accused.” *Doe v. United States*, 487 U.S. 201, 212 (1988) (internal quotation marks omitted) (emphasis in original). Accordingly, “[t]o qualify for the Fifth Amendment privilege, a communication must be [1]

testimonial, [2] incriminating, and [3] compelled.” *Hiibel v. Sixth Judicial Dist. Court of Nevada*, 542 U.S. 177, 189 (2004).

Here, there can be no question that Appellee’s disclosure of his password and decryption of his iPhone’s contents were compelled. The military judge so found, and this finding “rests on [the] determination of factual issues” and thus cannot be overturned “unless it has no support in the record.” *United States v. Doe*, 465 U.S. 605, 613–14 (1984). Only badgering by military investigators, in violation of his right to counsel, while Appellee was detained in his company commander’s office and under orders to comply with the investigators’ requests caused Appellee to relent and accede to their demands that he disclose his password and decrypt the contents of his iPhone. This is the hallmark of “compulsion.”

The pertinent issues, then, are whether the two separate sets of disclosures the government compelled Appellee to make are both “testimonial” and “incriminating.” A communication is “testimonial” (or, stated differently, “communicative,” *see, e.g., Schmerber v. California*, 384 U.S. 757, 761 (1966)) if “it[], explicitly or implicitly, relate[s] a factual assertion or disclose[s] information.” *Doe v. United States*, 487 U.S. 201, 210 (1988). The communication need not be damning in itself—the proverbial “smoking gun”—in order to be “incriminating;” rather, it is enough that the communication “would

furnish a link in the chain of evidence needed to prosecute the claimant.” *Hoffman v. United States*, 341 U.S. 479, 486 (1951); *see also, e.g., Maness v. Meyers*, 419 U.S. 449, 461 (1975) (“The protection does not merely encompass evidence which may lead to criminal conviction, but includes information which would furnish a link in the chain of evidence that could lead to prosecution, as well as evidence which an individual reasonably believes could be used against him in a criminal prosecution.”).

Each of these essential elements is satisfied here. The compelled disclosures Appellee made were testimonial in nature. Disclosure of the secret password needed to unlock Appellee’s iPhone was testimonial—no different than forcing a suspect to divulge from memory the combination to a locked safe. Similarly, compelled decryption of files in an iPhone or other encrypted device, without which the files are unintelligible, involves recreating on the device contents otherwise contained only in the suspect’s mind. These disclosures, either alone or in combination, are unquestionably incriminating because they formed links in the chain of evidence which led to the incriminating decrypted content obtained on the device. Accordingly, as the military judge correctly concluded, these compelled disclosures violated the privilege against self-incrimination.

A. *Just As Disclosure from Memory of the Combination to a Locked Safe Is Testimonial, So, Too, Is Recall and Disclosure of the Password to a Locked Electronic Device.*

As Appellee was detained in his commanding officer's office, he was forced to surrender to investigators the iPhone he had in his possession at the time. Taking physical possession of the device, however, did the investigators no good whatsoever because, like most iPhones and many other electronic devices in this time of hacking and other cyber threats to privacy, the device was password-protection *and* encrypted—and thus impervious to use or examination by anyone other than Appellee.

In order to act on its hunch that the iPhone might contain evidence that could be used to convict Appellee, the government needed a vital piece of information: the device's password. That information was available only from one source—Appellee—and it was contained in his memory. As long as the password safely remained hidden in Appellee's mind, the government could not extract any information (incriminating or otherwise) from the phone. The investigators could cobble together a case against Appellee only by getting him to disclose his password and thus reveal the contents of his mind, in derogation of his inviolable right to the privacy of his own thoughts.

This is the very definition of a testimonial or communicative act. As the Supreme Court held in *Doe v. United States*, “[t]he expression of the contents of

an individual's mind' is testimonial communication for purposes of the Fifth Amendment.” 487 U.S. 201, 210 n.9 (1988) (quoting dissenting opinion of Stevens, J.) (emphasis added). The portion of the Stevens dissent specifically endorsed by the *Doe* majority argued that an accused cannot “be compelled to use his mind to assist the prosecution in convicting him of a crime,” giving as an example of such prohibited compelled mental assistance the compulsion “to reveal the combination to his wall safe—by word or deed.” *Id.* at 219 (Stevens, J., dissenting).

“ The password to Appellee’s locked iPhone—like the example of the wall-safe combination from *Doe*—is hidden within the suspect’s mind. To allow criminal investigators to extract such information from the private recesses of the mind of the accused, against his will, would compel him to use his mind to assist in his own prosecution. This is the very self-condemnation the Fifth Amendment prevents. As *Doe* makes clear: “It is the ‘extortion of information from the accused,’ the attempt to force him ‘to disclose the contents of his own mind,’ that implicates the Self-Incrimination Clause.” *Id.* at 210 (majority opinion) (citations omitted) (first quoting *Couch v. United States*, 409 U.S. 322, 328 (1973), and then quoting *Curcio v. United States*, 354 U.S. 118, 128 (1957)).

These principles refute Appellant’s effort (Appellant’s Br. 15) to analogize coerced password disclosure to “be[ing] forced to surrender a key to a strongbox

containing incriminating documents.” *Id.* at 219 (Stevens, J., dissenting). Appellant is correct that the *Doe* majority and the Stevens dissent concluded that handing over the key (as opposed to divulging the password) to a safe would ordinarily be nontestimonial. *Id.*; *see also id.* at 210 n.9 (majority opinion). Unfortunately for Appellant, however, it misses the entire point of the Court’s discussion of how passwords differ, for self-incrimination purposes, from keys to safes.

Handing over a key is a physical act which does not require using the accused’s mind in any way. It discloses or communicates no information known to the accused but, rather, merely transfers possession of an object. Such a noncommunicative physical act in no way resembles forced disclosure of a secret password known only to the accused and hidden in the confines of his mind.

The Court’s decision in *United States v. Hubbell*, 530 U.S. 27 (2000)—a decision authored, notably, by Justice Stevens—reaffirms the critical distinction Appellant here misapprehends. Returning to the password-versus-key discussion from *Doe*, *see id.* at 43, *Hubbell* ruled that “there is a significant difference between the use of compulsion to extort *communications* from a defendant and compelling a person to *engage in conduct* that may be incriminating.”² *Id.* at 34—

² *But see Florida v. Stahl*, 206 So. 3d 124, 135 (Fla. Dist. Ct. App. 2016) (rejecting *Doe* and *Hubbell* on this point). *Stahl* overruled a Fifth Amendment

35 (emphasis added). Compelling disclosure of an iPhone password (or safe combination) committed to memory is in the former, testimonial category; the physical act of transferring possession of a key is in the second, nontestimonial category.

In light of *Hubbell*, it comes as no surprise that the lower federal courts have recognized that forced disclosure to the government of passwords necessary to access the incriminating contents of locked electronic devices or media would constitute self-incrimination. See, e.g., *SEC v. Huang*, No. 15-269, 2015 WL 5611644 at *2 (E.D. Pa. Sept. 23, 2015) (denying government motion for order compelling several accused to disclose their cellular passwords, on ground that such disclosure would reveal the accused's "personal thought processes" and constitute an "intrusion into the[ir] knowledge"); *United States v. Kirschner*, 823 F. Supp. 2d 665 (E.D. Mich. 2010) (similar).

The Eastern District of Michigan's decision in *Kirschner* is particularly instructive here. In that case, the government sought to compel the defendant to

objection to an order compelling an accused to divulge his iPhone passcode, finding the Supreme Court's distinction between a key to a safe and a combination passcode unconvincing. The court stated: "We question whether identifying the key which will open the strongbox—such that the key is surrendered—is, in fact, distinct from telling an officer the combination." The obvious explanation is the one the Supreme Court gave in *Hubbell*: "extort[ing] *communications* from a defendant" require the use of his mind, unlike "compelling a person to *engage in conduct* that may be incriminating." 530 U.S. at 31 (emphasis added).

disclose all of the passwords associated with his computers and files. 823 F. Supp. at 666. The court applied ordinary Fifth Amendment principles, not the act-of-production doctrine, stressing that “[t]his case is not about producing specific documents—it is about producing specific testimony [identifying his password].” *Id.* at 669. The court quashed the subpoena because “requiring [the defendant] to divulge through his mental processes his password” would be both testimonial and incriminating. *Id.* Exactly so, here, too.

Hubbell provides even further support for the view that disclosure of a passcode or combination is communicative in a way that performing a physical act is not. The case involved a subpoena commanding the accused to search through all of his documents for certain specified types of incriminating records, cull all responsive documents, and provide them to the prosecution. *Hubbell*, 530 U.S. at 31. The Court upheld the claim of Fifth Amendment privilege, concluding that the assistance the prosecution sought from the defendant called for a testimonial response. *Id.* at 45.

Among the reasons the *Hubbell* Court cited for its conclusion was that “the prosecutor needed [the accused’s] assistance” to obtain the incriminating information sought. *Id.* at 41; *see also id.* at 42 (adding that the prosecutor could not obtain the information required to convict without the accused performing “the mental and physical steps necessary” to provide it). Not only did the prosecutor’s

demand make it “necessary for [the accused] to make extensive use of the contents of his own mind,” but the prosecutor depended on a “truthful reply” by the accused in order to obtain the incriminating evidence. *Id.* at 43. This is in sharp contrast to truly nontestimonial acts (such as providing fingerprints, handwriting exemplars, blood samples, or keys to a locked safe), where no mental effort or truth-telling by the accused is required because the physical evidence the government obtains speaks for itself.

In this case, it is clear that the government needed Appellee’s truthful response in order to get the incriminating content it believed might be found on his iPhone. When the investigators interrogated him about his password, they clearly were asking him to search the recesses of his mind and give them his *actual* password, not a fictitious one. If Appellee had misled them by giving them a *false* password, or by claiming to have forgotten the password, the government would have obtained no information from the iPhone to build its case against him. It was only his truthful disclosure of his password that led to the discovery of the information the government needed to prove its suspicions of guilt, and such compelled disclosure constituted a testimonial communication under *Hubbell*.

B. *It is Irrelevant that Appellee Did Not Explicitly Disclose His Passcode Through Spoken or Written Word Because Entering the Code Directly into the iPhone Produced the Same Testimonial Result.*

To get around the substantial body of well-reasoned cases holding that compelled disclosure of passwords for locked electronic devices is testimonial, Appellant seeks to elevate form over substance. Conceding (as it must) that suppression would have been warranted had Appellee verbally told the investigators his passcode or written it down for them (Appellant’s Br. 12), Appellant argues that it is critical that Appellee disclosed his password in another, equally efficacious way: by entering it directly into his device (Appellants Br. 13–16). This, however, is a distinction without a constitutional difference. As Justice Stevens noted in his *Doe* dissent, a person may not be “compelled to reveal the combination to his wall safe—*by word or deed.*” 487 U.S. at 219 (emphasis added).

As an initial matter, Appellant’s exercise in splitting hairs ignores the reality of what transpired during the interrogation in this case. Once the investigators seized his iPhone, they immediately demanded that he *tell them* his passcode. (JA 405, 480). When Appellee refused, they resorted to an alternative means of getting him to disclose exactly the same information—namely, asking him to enter the passcode directly into the iPhone and to disable the password protection (JA 406,

480).

Two different investigative methods were used in an unrelenting effort to overcome Appellee's resistance, but they had exactly the same goal. That goal was two-fold. The first objective was to extract the secret passcode hidden in the recesses of his mind, exposing information which would otherwise remain hidden from all except Appellee. The second was to permit investigators to exploit the disclosure of the password from Appellee's mind in order to access the content on the device whenever they wanted in a search for evidence to use against him.

Because the two investigative methods were "functional equivalent[s]," they should be treated identically for "testimonial" purposes. *Cf. Hubbell*, 530 U.S. at 41–42 (treating a subpoena commanding the accused to look for and produce specified documents as "the functional equivalent of the preparation of an answer to either a detailed written interrogatory or a series of oral questions"). Given that Appellant concedes that it would have been testimonial if Appellee had acceded to the investigators' demand to tell them his password, the same result should obtain from the alternative yet equivalent disclosure method Appellee was forced to use.

Under settled law, what matters on the "testimonial" or "communicative" point is *not* whether the government received the information, but rather whether—as was certainly the case here—information was extracted from the mind of the accused. The Supreme Court could hardly have been clearer on this point in *Doe*

v. United States, 487 U.S. 201, (1988): “It is the ‘extortion of information from the accused,’ the attempt to force him ‘to disclose the contents of his own mind,’ that implicates the Self-Incrimination Clause.” 487 U.S. at 210; *see also id.* at 210 n.9 (“‘The expression of the contents of an individual’s mind’ is testimonial communication for purposes of the Fifth Amendment.” (quoting dissenting opinion of Stevens, J.)).

A simple hypothetical illustrates why Appellant’s form-over-substance argument should be rejected. Suppose the investigators had taken Appellee to the local Apple store and instructed him that, if he would not tell them his password, he should tell the store employee his password so that he could access the device. Appellee complies, and the employee unlocks the phone and, at the request of the investigators, disables the password protection. The investigators then reclaim the phone, search it, and find the incriminating content.

In the hypothetical, as here, the government can claim it never knew Appellee’s password. Nevertheless, it defies reason that forced disclosure of the password to a third party would be viewed as anything but compelled self-incrimination. In both cases, the lack of specific disclosure of the password to the government does not change the fact that the act of unlocking required extracting information contained in the Appellee’s mind and, consequently, formed a link in the causal chain leading to the discovery of the incriminating evidence on the

device. A disclosure can thus be “testimonial” even if the government was unaware of the specific facts extorted from the accused’s mind.³

This Court should follow Fifth Circuit precedent establishing that compelling an accused to use a code to unlock a device, as opposed to disclosing the code to the government, is testimonial. In *United States v. Green*, 272 F.3d 748 (5th Cir. 2001), the defendant was charged with illegal gun possession after investigators compelled him to enter the combination to his gun safes and discovered the firearms stored inside. Although the government never actually learned the combinations, the court of appeals dismissed as “without merit” the argument that entry of the code into the safe was nontestimonial. *Id.* at 753 (ruling that “Supreme Court precedent forecloses any argument that Green’s . . . opening the combination locks were not testimonial acts” and that entering the codes “so express[ed] the defendant’s mind as to constitute compelled self-incriminatory statements”).

³ Of course, if the government was not merely unaware of the specific facts communicated by the Appellee but truly in no position to exploit the disclosure for investigative gain, then the communication would not be causally linked to the discovery of incriminating evidence. So, for example, if an investigator called his colleague at the Apple store and told him to have the Apple employee re-engage password-protection because investigators had learned the password from an independent source, the forced disclosure of the password to the Apple store employee was compelled and testimonial, but not incriminating. In this case, of course, it cannot be disputed that the government could not have learned iPhone’s content but for the compulsion applied to Appellee to get him to unlock the phone.

In light of *Green*, it is irrelevant that Appellee entered his passcode directly into his iPhone rather than speaking it or writing it down. Each functionally equivalent form of expression required the use of the contents of his mind, the touchstone of a testimonial communication. The very act of having the passcode extracted from Appellee's mind by the investigators rendered it testimonial despite the government's claimed lack of specific knowledge of the contents of Appellee's communication.

II. DECRYPTION OF ENCRYPTED DEVICES OR MEDIA IS TESTIMONIAL BECAUSE IT RECREATES ON THE UNENCRYPTED DEVICE CONTENT THAT OTHERWISE EXISTS ONLY IN THE ACCUSED'S MIND.

The conclusion that the Appellee was compelled to make testimonial communications is only strengthened by the fact that the iPhone's contents were encrypted. As amici EFF and ACLU demonstrate, the process of encryption fundamentally changes the contents of the device by "transform[ing] data into a scrambled, unintelligible format." (Br. of EFF and ACLU 6). Without the decryption key, the data "exists *only* in its scrambled format." *Id.*

As a result, when the investigators seized Appellee's encrypted iPhone, *none* of the incriminating information they sought existed on the device. The contents of the device were hopelessly scrambled, entirely unusable to the investigators or anyone else in that format—and existed in unscrambled, intelligible form *only* in

Appellee's mind. In order to recreate the unscrambled information contained in the recesses of Appellee's mind, the government had to extract from it an additional piece of information: the decryption personal identification number ("PIN"). Without that vital piece of information, it would be as if the device's contents were written in a language known only to Appellee and could be rendered intelligible by others only if he were to translate it for them—which, of course, would require him to make extensive use of his mind.

Given that decryption translates encrypted content into a form anyone might understand—recreating the unscrambled information otherwise present only in the mind of the owner of the device—decryption is a testimonial communication. As explained by amici EFF and ACLU: "Translating unintelligible data via decryption communicates the content and characteristics of each and every file within the encrypted space. Indeed, it communicates whether any files exist at all." (Br. of EFF and ACLU 15 (citing *Hubbell*, 530 U.S. at 43).

The leading authority discussing whether decryption is testimonial, the Eleventh Circuit's decision in *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (2011), comes down squarely on the "testimonial" side of the question. Harkening back to the Supreme Court's familiar distinction in *Hubbell* and *Doe* between producing a key to a safe and disclosing the combination to a wall safe, the court of appeals held that decrypting a device "is more certainly

more akin to requiring production of a combination because both require the use of the contents of the mind.” *Id.* at 1337. Thus, to compel decryption is to force the device’s owner to give testimony and thus expose himself to incrimination.⁴

Although the Eleventh Circuit reached the right result on the “testimonial” issue, it should be noted that decryption would appear to be *even more strongly* testimonial than the forced disclosure of the combination to a safe. After all, even while a wall safe is locked, its contents exist in the same form they always had. Opening the safe merely allows ready access to its contents but those contents remain in exactly the same form as when the safe is locked.

Not so with decryption. Encryption changes the essential nature of the contents of the device, transforming content into a form incomprehensible to all except the person who knows the decryption PIN. Decryption has equally transformative effects but in the opposite direction: decryption uses the content of the device owner’s mind to recreate, out of essentially gibberish, intelligible

⁴ The source of the incrimination in *Doe* was not the unencrypted contents of the device because the court of appeals addressed the issue under the act-of-production doctrine. Other courts have taken the same approach as the Eleventh Circuit, agreeing that forced decryption is testimonial for act-of-production purposes. See *United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012); *In re Boucher*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009); *Commonwealth v. Gelfgatt*, 11 N.E. 3d 605 (Mass. 2014). That some of these decisions ultimately rejected the Fifth Amendment claim based on the “foregone conclusion” doctrine does not diminish their support for Appellee on the “testimonial” issue. Foregone-conclusion analysis has no application to self-incrimination challenges not based on act of production.

content mirroring the contents stored in the memory banks of the owner of the device.

If, as the Supreme Court has ruled, forced disclosure of the combination to a wall safe is “testimonial,” *see, e.g., United States v. Hubbell*, 530 U.S. 27, 43 (2000), it follows, *a fortiori*, that forced decryption of a device is as well.

III. THE FORCED DISCLOSURE OF APPELLEE’S SECRET PASSWORD AND FORCED DECRYPTION OF HIS LOCKED IPHONE WAS INCRIMINATING.

The last issue—one not open to serious question here—is whether, assuming disclosure of the iPhone’s password and decryption of its contents were “compelled” and “testimonial,” those communications were also “incriminating.” Clearly, the answer is yes. Under the act-of-production doctrine, the incrimination cannot come from the physical evidence the government seeks to obtain, but only from express or implied factual statements contained in the very act of producing the evidence. This, however, is decidedly *not* the case under ordinary Fifth Amendment principles.

It has “long been settled” that the “protection [of the Privilege] encompasses compelled statements that lead to the discovery of incriminating evidence even though the statements themselves are not incriminating and are not introduced into evidence.” *United States v. Hubbell*, 530 U.S. 27, 37 (2000). This principle traces

back to *United States v. Hoffman*, 341 U.S. 479, 486 (1951), which held as follows: “The privilege afforded not only extends to answers that would in themselves support a conviction under a federal criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute.” *See also, e.g., Kastigar v. United States*, 406 U.S. 441, 445 (1972) (ruling that the Fifth Amendment precludes both use and derivative use of compelled testimony to convict and that therefore only use-and-derivative-use immunity can abrogate a witness’s privilege against self-incrimination).

In this case, even if Appellee’s disclosure of his passcode and decryption of his iPhone’s contents were not, in themselves, incriminating, they most certainly were “links in the chain” leading to the discovery of the incriminating content contained on the device. *See In re Grand Jury Subpeona Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2011).

Confronted with a situation in which the government found incriminating evidence on the defendant’s computer after he was ordered to decrypt the drive, the Eleventh Circuit held that “even if the decryption and production . . . themselves are not incriminatory, they are a ‘link in the chain of evidence’ that is designed to lead to incriminating evidence; this is sufficient to invoke the Fifth Amendment privilege.” *Id.* at 1337–38. The same result is required here.

In fact, this case is an even stronger “link in the chain” case than the

Eleventh Circuit's. Entry of the passcode and decryption the contents of Appellee's mobile device were *indispensable* links in the chain leading to the discovery of the incriminating unencrypted content discovered on the phone. The unencrypted contents of SGT Mitchell's phone did not appear in the investigators' hands "like manna from heaven." *Hubbell*, 503 U.S. at 42. It was only through Appellee's "truthful reply" to the investigators request for his passcode and decryption "that the [g]overnment received the incriminating documents." *Id.* Had those two compelled communicative acts not taken place, the government would not have been able to find and use the incriminating content against Appellee.⁵ Accordingly, this Court should rule those acts to be incriminating and thus subject to the privilege against self-incrimination.

⁵ While the Army investigators questioning Appellee told him that if he did not provide his PIN, forensics examiners would unlock it, this was not true. Neither the Army Criminal Investigations Laboratory (JA 271) nor any commercial vendor (JA 317) can unlock and decrypt an iPhone 6. The necessary technology simply does not exist at this time.

CONCLUSION

The military judge was correct in finding a Fifth Amendment violation on this record, and her judgment should be affirmed.

Respectfully submitted,



DOMINIC X. BARCELEAU*

J.D. Candidate

Notre Dame Law School

Notre Dame, IN 46556

(781) 910-9477

dbarcele@nd.edu



STEPHEN F. SMITH*

Professor

Notre Dame Law School

3162 Eck Hall of Law


Notre Dame, IN 46556

(574) 631-3097

*Motion for admission to practice
pro hac vice pending

CERTIFICATE OF COMPLIANCE WITH RULE 24(d)

I certify that this brief complies with the type-volume limitation of Rule 24(d) because it contains 5773 words and has been prepared in a monospaced typeface using Microsoft Word 2013 with 14 characters per inch using Times New Roman font.

A handwritten signature in black ink, appearing to read 'D. Barceleau', with a long horizontal line extending to the right.

DOMINIC X. BARCELEAU*

J.D. Candidate

Notre Dame Law School

Notre Dame IN 46556

(781) 910-9477

dbarcele@nd.edu

*Motion for admission to
practice *pro hac vice* pending

CERTIFICATE OF FILING AND SERVICE

I certify that, on this 21st day of March, 2017, I caused a copy of the foregoing Amicus Curiae Brief of Notre Dame Law Student in Support of Appellee to be delivered to the Court, to the Army Government Appellate Division and the Army Appellate Defense Division.

A handwritten signature in black ink, appearing to read 'D. Barceleau', written over a horizontal line.

DOMINIC X. BARCELEAU*

J.D. Candidate

Notre Dame Law School

Notre Dame IN 46556

(781) 910-9477

dbarcele@nd.edu

*Motion for admission to
practice *pro hac vice* pending